LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-469514

Report of On-Site Inspection Workshop-18

J. J. Sweeney

February 8, 2011

Disclaimer

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Distr.: LIMITED
Draft WS-18 Report
XX December 2010

ENGLISH ONLY

CTBTO PREPARATORY COMMISSION | preparatory commission for the comprehensive nuclear-test-ban treaty organization

REPORT OF ON-SITE INSPECTION WORKSHOP-18

Technical Issues on the Draft On-Site Inspection Operational Manual

(Vienna, Austria, 22 – 26 November 2010)

Head of Organizing Committee:
Oleg Rozhkov

Co-Chairpersons:
Oleg Rozhkov, Malcolm Coxhead, Vitaly Shchukin

Rapporteur: Jerry Sweeney

Subject Leaders:
Malcolm Coxhead, John Walker, Wang Jun,
Gordon MacLeod, Vitaly Shchukin, Matjaz Prah

Summary

Several objectives were realized by this workshop: discussion of several technical issues related to development of the On-Site Inspection (OSI) Operational Manual; discussion of issues related to the list of OSI equipment, and introduction of and discussion of the PTS planning concept in preparation for and conduct of the next integrated field exercise.

Technical discussions related to the OSI Operational Manual included the topics of data handling and confidentiality, communications, and equipment-related inspection activities.

Based on presentations by PTS staff, the data handling and confidentiality discussions dealt with the preparation of data prior to an inspection and types of data to be included, as well as the integrated information management system (IIMS) that is currently being developed by the PTS. A key issue discussed in this area was the current three-level classification system called for by the OSI Operational Manual Model Text and implications for use of such a system and protection of information. These issues have important implications for the IIMS. There was also extensive discussion of technical and procedural issues related to the use of photography and the particular topic of digital photography and handling and authentication of digital images. One conclusion in this area is that digital photography should be a subject for future workshops and that the handling of digital photographic media should be consistent with Treaty provisions, especially with regard to the first generation product. Another conclusion is that there is a need to review the current text of the OSI Operational Manual.

Communications issues were discussed in the context of current work by the PTS, including recent experience from the directed exercise held in November in Jordan. A number of technical options were presented by the PTS and discussion focused on types of communication needed during an OSI and areas where secure communications and encryption might be needed.

Discussion of equipment-related pre-inspection activities focused on the various types of equipment lists that might be needed (with special distinction for the approved list of equipment by the Conference of States Parties), the uses of the different lists and how they are related, the level of detail needed, how to define core and auxiliary equipment, and issues related to equipment software. Much of this discussion continued during the session concerned with the equipment list itself, its structure and content and how functional/operational requirements and specifications should be developed. A presentation outlining the relevant equipment-related templates of the Organisation for the Prohibition of Chemical Weapons (OPCW) pointed the way for some possible approaches to equipment development for the OSI regime. A recommendation was made to use an approach similar to that of OSI Workshop-6 as a way to use expert groups to help develop the list of equipment.

OSI Director Rozhkov presented the PTS planning concept for and conduct of the next integrated field exercise. In the discussion that followed, noble gas collection and analysis were identified as a key priority for development along with the important need for a detailed realistic and scientifically credible scenario.

The numerous findings and recommendations from the five sessions of this workshop are listed at near the end of this report. In addition, results of this workshop will be incorporated by the WGB Task Leader for the OSI Operational Manual into a series of issue papers

containing articulated concepts on the issues covered. An initial version of these, titled "Suggestion Paper Provided by the OSI Operational Manual Task Leader" is included in this report.

Discussions during this workshop benefitted greatly from the experience base of the participants, both from the staff of the PTS and from participants representing States Parties. Many of the participants had participated in the 2008 integrated field exercise as well as later directed exercises sponsored by the PTS, such as the directed exercise in Finland (DE09), the 2009 noble gas exercise (NG09), and the 2010 directed exercise in Jordan (DE10). Other important experience brought to bear was that from the OPCW. This experience was reflected in the discussions, in the narrative of the five sessions below, and in the findings and recommendations that are found near the end of this report.

Contents

Abbreviations .....
Introduction .....

Proceedings
- Opening Remarks .....
- Session A: Inspection Team Data Handling and Confidentiality .....
  - Handling of Digital Images .....
- Session B: Inspection Team Communications .....
- Session C: Equipment-Related Pre-Inspection Activities .....
- Session D: OSI Equipment List .....
- Session E: Preparation for the Next IFE .....

Findings and Recommendations .....
- Session A: Inspection Team Data Handling and Confidentiality .....
- Session B: Inspection Team Communications .....
- Session C: Equipment-Related Pre-Inspection Activities .....
- Session D: OSI Equipment List .....
- Session E: Preparation for the Next IFE .....

Acknowledgements by the Rapporteur .....

Annex I List of Presentations .....
Annex II Suggestion Paper Provided by the Task Leader for the Draft OSI Operational Manual for Session A
Annex III List of Reference Material .....
Annex IV List of Participants .....

Abbreviations

BOO	base of operations
CPT	continuation period techniques
CSP	Conference of the States Parties
CTBT	Comprehensive Nuclear-Test-Ban Treaty ("the Treaty")
CTBTO	Comprehensive Nuclear-Test-Ban Treaty Organization ("the Organization")
CWC	Chemical Weapons Convention
DE	directed exercise
DG	Director-General
EC	Executive Council
ECS	Experts Communication System
EIF	entry into force
ESMF	Equipment Storage and Maintenance Facility
EU	European Union
HF	high frequency
GIS	geographic information system
GPS	global positioning system
IA	inspection area
IAEA	International Atomic Energy Agency
IDC	International Data Centre
IFE	Integrated Field Exercise
IIMS	integrated information management system
IMS	International Monitoring System
ISP	inspected State Party
IT	inspection team
MT	Model Text (for the draft OSI Operational Manual)
NATO	North Atlantic Treaty Organization
OPCW	Organisation for the Prohibition of Chemical Weapons
OSC	Operations Support Centre
OSI	on-site inspection
POE	point of entry
PMO	Policy Making Organ
PTS	Provisional Technical Secretariat
RSP	requesting State Party
SAMS	Seismic Aftershock Monitoring System
SOP	standard operating procedure
TID	tamper indicating device
TS	Technical Secretariat
TTBT	Threshold Test Ban Treaty
UHF	ultra high frequency
UNE	underground nuclear explosion
VCDR	Vienna Convention of Diplomatic Rights
VHF	very high frequency
VSAT	Very Small Aperture Terminal
WGB	Working Group B

INTRODUCTION

The principal goal of this workshop was to provide a forum for discussion of the specific topic areas of the OSI Operational Manual. In addition, sessions were also held to discuss the development of the OSI equipment list and to introduce and discuss the PTS planning and concept for the next integrated field exercise. For the OSI Operational Manual discussion, the focus was on data handling and confidentiality, communications, and equipment-related issues. The focus of these sessions was on technical and operational issues, with results of the discussions intended to provide the Task Leader for the OSI Operational Manual with articulated concepts to include in issue papers that could be discussed by Working Group B.

The organisation of the workshop was designed with a small number of short presentations, followed by discussion among participants. The intent was to provide as much time as possible for discussion, facilitated by the five subject leaders. The final day of the workshop consisted of a discussion of findings and recommendations that were developed by the subject leaders for each of the sessions.

The initial part of this report ("Proceedings") consists of a narrative of the presentations and discussions. The intent of this section is to provide the reader with a general sense of what was presented and the general flow of the ensuing discussions. This is followed by a listing, by session, of the findings and recommendations of this workshop. A list of presentations, as well as a suggestion paper provided by the Task Leader for the draft OSI Operational Manual on alternative data protection arrangements, can be found in the annexes, along with a list of reference materials and participant contact details.

A DVD containing OSI Workshop-18 documentation, including presentations, is available from the PTS on request.

PROCEEDINGS

OPENING REMARKS

Rozhkov introduced himself as the new director of the On-Site Inspection (OSI) Division and welcomed participants to the workshop. He described the current work of the OSI Division as continuation of the steady build-up of capabilities via implementation of the OSI Action Plan. He noted that Working Group B (WGB) is well into the third round of elaboration of the draft OSI Operational Manual, and its state of completion has a major impact on the work of the Provisional Technical Secretariat (PTS). He noted that, although it has a somewhat unique focus, this workshop is nevertheless a continuation of the previous 17 OSI workshops focused on development of procedures and equipment and providing support for the development of the OSI Operational Manual. He introduced the topics of this workshop, which also included introducing the PTS planning concept for the next integrated field exercise (IFE), which was covered towards the end of the workshop.

Shchukin, WGB Task Leader for OSI and co-chairperson of the workshop, introduced the objectives of OSI Workshop-18, which were to:

1. Clarify technical issues in the third round of elaboration of the draft OSI Operational Manual;
2. Provide contributions to the development of the list of OSI equipment; and
3. Contribute to the development of a conceptual approach to the planning and preparation for the next IFE.

Shchukin noted that the first objective concerned three main areas: data handling and confidentiality; communications; and equipment-related pre-inspection activities. A goal of the second objective was to review relevant knowledge, including earlier developments and experience from other treaties. For the third objective, the intent was to discuss an initial set of PTS suggestions for the planning and preparation of the next IFE. Outcomes of this workshop would be included in the workshop report, draft Task Leader papers, and a revised set of PTS suggestions for the next IFE. Finally, he emphasized that there is a synergy between the cluster of objectives for this workshop and the role for further development of OSI capabilities.

Coxhead, WGB Task Leader for the draft OSI Operational Manual, noted that previous workshops dealing with the OSI Operational Manual were focused on development of text. This workshop was a hybrid in the sense that it intended to focus on technical issues, with general discussion of concepts. The workshop would draw upon practical lessons from the IFE and directed exercises (DEs). He referred participants to handouts, which listed specific sections from the Model Text (MT) for the draft OSI Operational Manual, which were intended to a focus for the discussions. The intent was to review the provisions therein against the perspective of the participants, including the PTS. Coxhead also noted that he was in the process of preparing an updated version of the MT as discussed by WGB at its thirty-fifth session.

Coxhead outlined the method of work for the workshop. The Subject Leaders would introduce the subject for the relevant section of the workshop and this would be followed by a series of short presentations. As well as capturing the main workshop findings, the workshop report

would attempt to capture the issues and nature of the discussions that follow the presentations. The outcomes of the workshop as referenced in the workshop report should include articulated concepts that he (Coxhead, as Task Leader) would be able to take to be reflected in issue papers for consideration by WGB.

In her introductory remarks, Deng further refined the guidance on the method of work and announced the following subject leaders for the five sessions of the workshop:

Session A: IT Data Handling and Confidentiality – Malcolm Coxhead and John Walker
Session B: IT Communications – Wang Jun
Session C: Equipment-Related Pre-Inspection Activities – Gordon MacLeod
Session D: OSI Equipment List – Vitaly Shchukin
Session E: Preparation for the Next IFE – Matjaz Prah

SESSION A: INSPECTION TEAM DATA HANDLING AND CONFIDENTIALITY

Session A was introduced by Coxhead as co-subject leader for the session. He noted that Chapter 10 and other places in the Model Text provide current draft guidance on confidentiality and data handling. A major focus of this workshop would be how the PTS had been working to address the lessons of the 2008 OSI Integrated Field Exercise (IFE08). In addition, several other workshop presentations would cover these issues. Prospective issues for discussion at this workshop in the area of data handling and confidentiality concern:

- Section 5.4, which currently deals with division of the Base of Operations (BOO) into different activity areas;
- Arrangements for classification of information gathered in the inspection area (IA) (paragraphs 10.4.12-10.4.16);
- Need to know issues (paragraph 10.4.20] based on classification of information and data;
- Data protections (Annex 3.1) for practical procedures for protecting information and data;
- Other Model Text topics, such as handling of photographic data (paragraph 6.7.3(d)] and joint storage (paragraph 10.4.24).

Balczo began the technical presentations by introducing two presentations concerning data handling given by PTS staff members. He noted that experience from IFE08 and the clear need to deal with various issues related to the build-up for the next IFE have led to the identification of specific issues of data handling and confidentiality that need to be addressed, either within the MT or possibly in a "Confidentiality Handbook".

Presentation: Ciganikova: "Data Handling During the Pre-Inspection Period"

Ciganikova reviewed the tight timeline associated with preparation for an OSI, which is dominated by the six-day period in which much of the data needed to carry out the OSI must be prepared. Timeline considerations suggest that certain types of data should be assembled beforehand. A key question to be resolved was where the information will come from that will be used during an OSI. She provided a list of the types of information that should be included, such as data concerning the triggering event, boundaries of the inspection area (IA), information from the requesting State Party (RSP) or other State Party, topographical, geophysical, and geological maps, as well as the country file that provides background information such as climate, politics, and seismic history. Sources of the information proposed by Ciganikova were an OSI databank, the RSP, inspected State Party (ISP), other State Parties, and from the International Monitoring System/International Data Centre of the CTBTO (IMS/IDC).

She discussed the development of the databank for OSI, an activity that was part of the current PTS action plan. Example tables of information that the PTS had identified as relevant requirements were presented that included data items such as country profiles and standing arrangements. In addition, there were different modules for geographical information systems (GIS), personnel, budget and finance, equipment and storage, and environmental health and safety. The next steps would be to identify the actions needed to organize the data, identify the information requirements, and then to group the information requirements into models for

the databank. Ciganikova reviewed other possible inputs to the databank, such as data related to the consultation/clarification process; confidence building measures, cooperative national facilities, and national technical means (NTM). In some cases the information might be confidential. She also addressed other issues, such as the need for a common format for data that can be used by the Technical Secretariat (TS) and the important reality that some data coming from the IMS/IDC pipeline (such as results from radionuclide laboratory analyses) might not be available within the six-day preparation period. She finished the presentation by showing an example of the development of an initial inspection plan based on using the databank.

Presentation: Labak: "Integrated Information Management System and Data Handling During an OSI"

Labak reviewed the goals and status of current development of an integrated information management system (IIMS) by the PTS. He noted that, during an OSI, the inspection team (IT) conducts activities and needs to document findings in the form of the preliminary findings document. A need to support the continuous flow of activities and daily operations during an OSI and integrating data collected and analyzed with daily operations pointed to the need for a data management tool. In addition to tasks such as logging activities and documenting their results, the IIMS would have to be able to provide the IT with visualization tools, capabilities for sharing data within the IT and with the ISP, integrating activities, providing management tools, dealing with ISP needs, and dealing with information protection requirements. One important issue was the process for entering data into the management system. Labak defined the concept of defining a receiving area and a working area and provided an example list of activities and objectives for each. He also reviewed some of the issues involved with classification and data access, referring to the three levels of protection outlined in the current MT. In his conclusion, Labak noted that the initial version of an IIMS developed by the PTS was to be tested during an exercise in Vienna the week of December 13, 2010. The current version took into account the possibility of handling a continuous flow of data as well as classified data.

Comments and Discussion

Ciganikova stated that the current concept for country profiles included in the databank for OSI preparation would contain only open-source information and information provided as part of standing arrangements. Other discussion of the preparation database revolved around how to determine data formats (e.g. maps scales, details of profiles), how to control data formats, and how these would be agreed upon. The important issue of the IMS/IDC pipeline was also discussed, especially the issue of if and how data produced by the pipeline after the startup of the inspection could be conveyed to the IT.

Most of the discussion about Labak's presentation and the IIMS revolved around the concept of the receiving area and the issue of protection of data, as well as the need to remove data from the system if later deemed not relevant to the OSI. One participant commented that, in addition to data, consideration should also be given to samples that are collected in the field. Issues remaining to be addressed include what is the nature of the receiving area where samples are concerned and at what point are analysis results entered into the IIMS, since there is a separate chain of custody for samples and results of the analyses of samples that must be stored. Other participants brought up the point that other types of data, such as visual

observation data (e.g., photographs, descriptions) also need to be considered for data entry; it is important to keep the system flexible to handle different data types. With respect to the review concept, it was pointed out that the concept of joint (IT and ISP) review of the data is needed and should be included in concepts of the nature of the receiving area. When asked whether the receiving area was a virtual area or a physical area, Labak replied that it is a physical area, separated from other activities. Finally, there was extensive discussion of the issue of when information might be deemed to be not relevant to the OSI. When and how this is done and what happens with data already in the system are important concepts for the design of the IIMS. Several participants noted that it is possible that relevancy for certain types of information might not be determined until well into the inspection and after the information is entered into the IIMS. This could be solved by requiring a mechanism for removing information from the system deemed non-relevant. or perhaps by having the understanding that the data would be returned to the ISP at the end of the inspection
.

Presentation: MacLeod: "OSI Confidentiality Considerations"

MacLeod reviewed current MT references related to confidentiality and relevant Treaty language. He pointed out a basic concept from the MT that data is "born" OSI limited. In other words, by default, data is assumed to be OSI Limited and action has to be taken to make data or information more limited. Under the Treaty, the ISP has a right to protect national security interests; this implies that it is important for the ISP to have people on hand during the inspection to make decisions about sensitivity of information and data. Distinctions about sensitivity should be made in the field before it arrives back to the base of operations (BOO).

MacLeod noted there were three different levels of information security called for in the MT; he pointed out that it was important to realize that at each level protocols are needed for marking the data and how it should be handled. Applying a classification invokes certain obligations about protection and how data should be handled as paper records and within an electronic database. For example, different levels of classification should not be mixed into the same computer system. Another issue was how different classification levels for samples should be handled – ideally, separate storage and analysis systems are needed at each level of classification. All of these issues have certain impacts on the IIMS; the more equipment that is needed, the more people that are needed to operate it, along with larger facilities to house it, more power needed, etc. He also pointed out that need to know criteria create "stovepipes" – narrow channels of information transfer that limit the synergy within the IT that could limit team effectiveness. Finally, MacLeod brought up the issue of breaches to the classification system – how is classified data removed from a computer system? These issues also come up when the classification level of information is changed.

As an alternative to the three-level classification system inherent in the MT, MacLeod suggested to flip the idea of "born OSI Limited" and simply use a system in which everything is OSI Highly Protected and to which the entire IT has full access. With such a system there is no need to have duplicate systems it eliminates the possibility of breaches and system contamination.

Comments and Discussion

One participant commented that physical security would be very difficult at the BOO and wondered what would constitute a "serious" breach of security. Another comment was that, in the system currently outlined in the MT, classification was done jointly by the IT and the ISP and there was no automatic declassification; the preliminary findings document would be the highest classification. There was a further suggestion that breach of information issues should be covered somewhere other than in the OSI Operational Manual. One participant asked about Treaty guidance on declassifying information after an inspection; MacLeod answered that the Treaty was silent on this issue. In response to a question, he also said that in his concept the level of OSI Highly Protected applied to everything. As a summary of the discussion, Coxhead said that it might be useful to consider the concept of "handling" information at a certain level of protection, notwithstanding how it may have been classified, for the purposes of the OSI Operational Manual.

Presentation: Han: "Consideration on IT data handling and confidentiality"

Han stated that the goals for protection of OSI information are to gain the confidence and cooperation of the ISP and to facilitate the successful conduct of an OSI. To ensure this, all data should be saved in an unchangeable format every day, with joint storage by the IT and the ISP. He also recommended that encryption be employed for data transmission and storage and that wireless communication equipment and a writable optic driver should not be included in dedicated IT computers to prevent unauthorized access. A computer should not contain information higher than the classification of the computer. (This implies using separate computer systems for each level of classification.) He suggested that paper documents should have a chain of custody and that it might be necessary to have an IT member be responsible for document management.

Comments and Discussion

The issue of removal of data from archives if they had been reclassified or deemed non-relevant to the inspection was brought up – should they be removed from the archive? How should this be done with electronic storage? Re-qualification of data might require the re-qualification of the computer system on which they were stored. One participant wondered which documents would need to be protected.

Presentation: Osugi: "Confidential Issues for CTBT"

Osugi stated that fundamentally there is a clash of interests concerning rights and obligations in the Treaty that requires coordination between the IT and the ISP, implying that guidance should be provided in the OSI Operational Manual to facilitate it. He suggested that there was a need to avoid confusion between the terms "confidential" and "sensitive". Thereby, he divided information gathered in an OSI into two categories: category A, for which the TS took steps for confidentiality, and category B for which the State Party (including the ISP during an inspection) took steps for confidentiality. He suggested that the Director-General (DG) is the place where information classified by the SP may be deemed relevant and thus declassified and included in the final inspection report. (For information provided by the ISP, the DG could decide to declassify such information himself. For information provided by State Parties other than the ISP, the DG would need an agreement with the information

providers on the declassification).

Session Comments and Discussion

Coxhead. as subject leader for the session, led the session discussion by providing his summary of the presentations as follows:

The presentations covered the issues of:

- Handling and assembling information when the TS is preparing for an inspection (Ciganikova)
- Providing tools for handling information in the field and organizing information (Labak)
- The conundrum of how to deal with classification of information, specifically concerning the possible value of a simpler classification scheme (MacLeod)
- The need to have a clear trail of information and definition of responsible parties (Han, Osugi)
- Consideration of an approach used by the International Atomic Energy Agency (IAEA) in reference to the CTBT (but it is difficult to understand how it might apply).

Finally, he challenged the group to consider what sort of adjustments to the draft text should be considered.

The discussion of the need to know principle noted that it was currently based on having various levels of classification, but if separate levels are not used, need to know would not apply because all IT members would have the same information. General opinion of the group was that such a principle is probably acceptable or even to be desired that all IT members have access to the same information. A more fundamental question is whether the three levels of classification currently advocated in the MT should be retained. Many of the group suggested that the three level system currently proposed in the MT probably would not work in practice. The single classification system is more streamlined and minimizes opportunities for abuse. The subject leader asked if simplifying the system in this way was an attractive idea and suggested that a tabletop exercise might help to clarify the issue of how to classify information.

Further discussion focused on the core problem of how confidential information should be protected. The idea currently implied in the MT is that there should not be too much highly protected information. If everything is at the same level, the ability to single out certain types of information might be lost. This issue should be dealt with in specific cases, not in the abstract. Additional discussion concerned when a classification decision was made about information – some opinion was that this only occurred when the PFD goes only to the DG – and whether certain information could be withheld from some members of the Executive Council (EC).

Additional discussion revolved around technical aspects of protecting information and securely removing information with electronic storage. It is clear that Section A4 of the MT creates security requirements that may have to be multiplied by three if a three-level system of protection were to be used. Coxhead suggested that the procedures of the MT should be revisited and exercises carried out to ensure the practicality and functionality of data

management if highly protected became a common occurrence.

In regard to the issue of data protection. Coxhead suggested that a possible approach might be something based on an IIMS system with access controls and/or encryption. It is desirable to separate need to know from classification levels; every team member needed to access data and inspection results, but on occasion it might be allowable to limit access to very sensitive data. Coxhead suggested that this issue might be solved by introducing different mechanisms such as having the ISP negotiate the assignment of conditions or by limiting distribution; in this case protection would be defined via managed access rather than via a classification. Recognizing that these data protection issues have major importance for the OSI Operational Manual and implications for the development of the IIMS, Coxhead distributed a draft paper, titled "Suggestion for alternative data protection arrangements". A copy of this paper can be found in Annex II.

Handling of Digital Images

Walker, as subject leader, introduced the second part of Session A, which dealt with handling of digital images. He referred to the sections of the MT (Section 6.7, and paragraphs 4.3.13 (iii) and 6.2.6) that covered photography that were to be reviewed in the workshop. Walker reviewed experience from IFE08 and some of the procedures used for handling photography. As played during IFE08, the ISP put no restrictions on taking photographs. Back at the BOO, photos were later reviewed by the ISP and only a few were then determined to be confidential. These showed photos of boreholes and as such were classified by the ISP as Highly Protected, and could not be removed from the ISP's territory. This provoked IT objections as the team wished to include these photographs in its Preliminary Findings Document. This issue was unresolved in the IFE08 through lack of time in exercise play.

Walker referred to relevant lessons learned from IFE08 that included issues of associating global positioning system (GPS) data with photos, cases where frame numbers were missing in sequence, and problems with associating map coordinates with initial overflight photos. He noted that IFE08 experience provided much procedural information to help with the development of standard operating procedures (SOPs).

Referring to a list of questions for discussion, Walker questioned some aspects of the procedures used during IFE08. Some of the questions included: Is the log of photo file reference (JPEG) numbers (with shutter release count number) adequate? How should images be handled that are deemed to be confidential? The onus is on the ISP to control photography if it has concerns, so how much procedural information should be included in the operational manual? Other issues included relevance, joint storage access, facilities needed for review and storage, and how photography should be linked to maps. All of these issues should be included in procedures contained in SOPs.

Presentation: Arndt: "Handling of digital images and experience from forensic works"

Arndt introduced Christoph Kaltseis, a freelance photographer with expertise in forensic photography, who presented an overview of a commercial software package from Adobe and who shared some ideas about how forensic photography was applied. Kaltseis began by pointing out that with a digital single lens reflex camera (DSLR) the software could detect any changes to the original image. For cameras with high light sensitivity and range, post-processing could be used to enhance features on the image. Cameras could be designed to record raw images in dual, non-alterable cards within the camera. An important point he made was that saving raw files (at the bit level of data) was the most secure way to ensure that the image had not been tampered with. The JPEG file convention was a compressed mode from the original and with it some information was deleted. A shutter counter could detect changes to the memory card or missing images. The latest version of Adobe Photoshop®, version Cs5, can handle 16 bits per colour channel which (in the case of the red, green, and blue (RGB) channels) brings the information depth to 48 bits. If the operational mode is set to high dynamic range (HDR), the software is able to handle even 96 bits – which is the current state of the art in image processing. All changes to the original image are stored in an image file which is paired with a read-only tamper-proof text file that lists all the steps in processing leading to the image being viewed. Other special functions in the software check image alignment, can stack multiple images to check for changes and eliminate noise, and can allow for metering (making precise measurements of the dimensions of objects in an image). Kaltseis illustrated many of his points, including the concepts of image version tracking and use of metering methods (for estimating the size of a crater), with examples taken from IFE08 and from the recent DE10 in Jordan.

Arndt point out that, in order to use digital photography, SOPs will need to be meshed with procedures in the OSI Operational Manual. The retained original stored raw data file, which is authenticated using special software from the camera supplier, serves both sides as an absolute reference, which is more secure than analogue media (film photography). In addition, digital photography allows the IT to easily enhance specific features in order obtain more information from an image and enhance OSI capabilities.

Comments and Discussion

In leading the discussion, Walker started by outlining several general issues that could be covered:

1. Are the procedures contained in the MT adequate or about right?
2. What types of SOPs are required?
3. The concept of operations for photography should include issues like how many photos to take and for what purpose.
4. Guidelines should be included (in the MT or SOPs) for joint storage of original media and processing steps.
5. Guidelines should be included (in the MT or SOPs) for the role of hard copies of photos for inspection reporting.

In an initial comment, one participant noted that the MT still referred to older film systems; it needed to be changed so that the language was not specific to a particular technology (e.g. wet rooms and dark rooms). Walker noted that, in addition, the SOPs for photography and visual

observation would have to keep up with changes in technology, but the MT should stick to "principles" independent of technology. Another participant suggested that the definition of photography could be taken to include multispectral imagery, since some cameras can record in those spectral bands. In reply, Walker noted that photography, as he interpreted it, referred to the visible spectrum.

Concept of Operations for Photography

Several participants commented that the number of photos taken should probably be limited in practice – too many photos create problems of accounting, review, etc. – but this must be balanced against the possibility that certain photos might be the only chance to record a short visit to a particular place. Several purposes of photography could be envisaged, such as photos of sampling points or instrument settings as well as general reference and forensic photos. It would probably be useful to define all the uses of photography in an SOP as well as to prescribe an "inspection relevant culture". Other comments dealt with technology-related issues that should be considered, such as how to define the recording media, how to define or specify the software in the camera, what metadata should be included with raw photo data, and how to deal with failures of technology, such as when a GPS reference for a series of photos fails. Finally, one participant noted that many of these issues were considered in the current SOP for visual observation.

Role of Hard Copies for Photography

The main question considered was: "Is there a case for a hard copy of all images or should the IT rely on a specific technology?" A participant pointed out that, for the IIMS that was being developed by the PTS, hard copies of photos or documents were scanned for archiving so, in this case, a hard copy ended up being an electronic file. Another participant noted that during IFE08 each hard copy that was highly protected had to be signed and dated; this could be difficult to do for all photographs, especially if there were hundreds. Another person pointed out that the use of hard copy had logistical requirements – ink and paper at the BOO. Another point was that something close to the original image should be stored as a record, but printing copies should only be used as a tool for the work of the IT or for reporting. General consensus was that the system used should be practical and useful in the field and this should be reflected in the MT.

Issue of Joint Storage

Walker pointed out that joint storage was used in IFE08 for only a few copies of photos, and that confidentiality played a critical role. A participant noted that the OSI Operational Manual referred to joint seal/storage as part of the rights of the ISP; an important issue is how this should be dealt with within the IIMS. Another comment was that, in a database system, taking IT-owned items out from such joint storage can be a problematic issue; photographs determined to be sensitive might be allowed to be put into the database and stored separately. There is a need to review what is meant by joint storage – does it include physical separation as well as the way data is handled? Another issue brought up was the case when the ISP provided the photographers – the timing of photo release, how photos were handled, etc. and what is the meaning of joint seal if the ISP keeps the first generation of the photographs. It might be the case that the ISP wants to allow only limited release of photos to the IT. One participant summed up many of the issues by stating that the first layer is the ISP right to

retain the first generation product; the second layer is dual seal availability to both the ISP and IT; the best way to prevent disputes about retention is by agreeing on the photograph composition in the first place, when it is taken in the field. Again, a key element is the marrying of technology with the SOPs for visual observation and data handling.

Further discussion focused on some of the technical aspects of forensic cameras. One participant questioned whether a photographer provided by the ISP would be able to properly operate a camera provided by the TS. Kaltseis noted that the type of camera he described was capable of having general settings programmed into the camera software ahead of time, so that the operator would only have to point and shoot. Another point made was that there might be some role for the use of "ordinary" (e.g. non-forensic) cameras. A high technology camera could be used for a specific photographic record and other cameras could be used for general use and reference. All of these issues need to be considered in the concept of operations along with the need to protect integrity and confidentiality. These issues could be the focus of a specific future workshop.

Walker summarized the discussion by saying that there is a clear need to merge technology with the SOPs and in the general text of the MT. A special workshop on photography should be a recommendation of the workshop, and many of these concepts should be included in the inspector training for visual observation.

SESSION B: INSPECTION TEAM COMMUNICATIONS

Wang, as subject leader for Session B, introduced the communications concept with a diagram of communications flow, organized by elements of the OSI (e.g. the DG, EC, TS, IT, RSP) with lines between elements representing lines of communication. Another viewgraph provided a list of basic assumptions that he proposed the group try to reach agreement on:

- Redundancy of communications equipment with backup sets and alternate means.
- IT self-dependence and sufficiency for communication equipment at start-up, subject to later arrangements with the ISP.
- The range of operation of the equipment should be requirement driven and modified to fit possible scenarios.
- Lessons of the past can be of reference but should be open for the future to allow for possible technical improvements.
- A minimum threshold of communication standards should be established which will be the standard for negotiation with the ISP.
- Confidentiality issues should be minimized while maximizing safety and security factors (more back up and more margins for health and safety).

For the scope of the discussion, Wang suggested that the group review procedures but not text from the MT. Technical requirements from Annex A2.2 should be reviewed with a goal to identify further issues for elaboration. Technical concepts and specifications should be reviewed with an eye towards the next stage of development of the MT to be ready prior to the next IFE.

Presentation: Prah and Abushady – "Communication Testing during DE10"

The purpose of Prah's presentation was to review the communications requirements of the Treaty and the process of PTS development of communications capabilities for an OSI. He began by emphasizing the right, defined by the Treaty, of the IT members to communicate with each other and with TS. Not only is this an important aspect of the Treaty, it is also vitally important for health and safety. Prah noted that development of communications capabilities have been a continuing activity of the PTS, with testing of various aspects of communications during previous field tests and directed exercises in 2002, 2005, 2006, IFE08 and during the recent directed exercise, DE10, which took place in early November 2010 in Jordan. He outlined some of the different types of communications: between the IT in the field and the Operations Support Centre (OSC); within the IT; and communications during overflights between IT personnel on the plane and on the ground.

Some of the technical means being considered and tested were communications by satellite, cell phone and land lines, as well as communications provided by the ISP. Options for communications between the BOO and the team in the field that were being considered included high frequency (HF), very high frequency (VHF) and ultra high frequency (UHF) radios connected via a network or via satellite phones.

As an introduction for the following presentation by Abushady, Prah outlined the objectives of DE10 for communications, which were to test synergy and communications concepts and hardware solutions for OSI and provide base level experience for development of SOPs for

communications. He noted that, for DE10, an area was chosen with rugged terrain in order to provide realistic challenges to OSI communications.

Abushady reviewed equipment aspects of the DE10 communications exercise. He described seven different communications systems that were tested and provided assessments of how they performed. The Iridium satellite system provided on demand calls and was relatively easy to set up and use, but the system was expensive to operate, and there was no GPS capability. This system would be recommended for use only as a backup. The Inmarsat BGAN broadband system had the advantages of small size and short setup time; it was good for data transmission but was also expensive. This system was also recommended as a backup. The Very Small Aperture Terminal (VSAT) system had a high investment cost, took time to set up and had relatively large size, but it was highly reliable and stable and inexpensive to use. This system was recommended as the primary means for OSI communications.

Abushady noted that because of technical difficulties at headquarters in Vienna, it was not possible to test secure communications fully during DE10. However, it was possible to test some secure communications incorporating cellular and land line connections. The Sectra Tiger XS was found to be a good system for secure communications between the inspection team leader (ITL) and the DG. The SPOT personnel tracking devices operated within a vehicle and were inexpensive, but they needed an active data connection for viewing locations of the units. This system was also recommended as a backup. A system developed by the CTBTO, called the CTBTO flightcase solution, utilized long distance (HF) and short distance (UHF) communications for tracking units. By means of links between the HF and UHF systems, all units could be tracked. Abushady pointed out that modern digital systems had the advantages of being able to track people as well as give priority to voice (UHF islands were connected to each other and base via HF). An alternative solution to ground-based systems was to use satellite instead of HF on the ground; in this case repeaters and antennas were not needed. He described the hybrid system of HF and UHF radio combined with satellite connection that was the current system favoured by the PTS and showed examples of some of the hardware and display systems. In summary, he said that the solution worked and the digital UHF added certain capabilities, but more testing was needed to address issues such as HF interference, antennas, and packaging/physical design issues.

Comments and Discussion

In response to a question, Prah said that by tuning the antennas, 90% radio coverage could be achieved in areas of rugged topography and this could be adapted by relaying messages via other vehicles. Prah also added that the tracker devices included an emergency alert capability and that this technology was changing rapidly. On encryption, Prah said that UHF radios had encryption capability, but not at the level of secure devices. When asked how ready the PTS was to develop equipment specifications, Prah said that they should be ready by the end of 2011 for another test. One participant pointed out that the PTS needed to establish a set of minimum requirements for the type of communication system that the ISP should provide. Another participant noted that communications procedures were another important issue, and Prah replied that the PTS had started development of draft procedures.

Wang summarized the discussion as follows:

- Significant progress in communications development has been made.
- A standardized requirement for communications should be updated and proposed by the PTS.
- Policies regarding the use of communications are needed, including a minimal set of requirements (including security, and health and safety) in the form of SOPs or at a higher level.
- Specifications for communications equipment need to be developed.

Presentation: Gordon MacLeod "OSI Communications"

MacLeod started with a review of the Treaty and Protocol and language concerning rights to use secure communications and the right of the IT to communicate with each other and with the TS. He referred to the current MT language as having two "flavours" – one level it describes how some communications are to be accomplished, but it also modifies the Treaty by creating certain caveats and restrictions not found in the Treaty or the Protocol. He pointed out that, since the ISP would provide the means for communication during an OSI, there is in reality no need to invoke restrictions in the OSI Operational Manual. MacLeod followed this up by providing an example of how the ISP and the IT could work together to arrange that communications meet the functional requirements of the IT. He proposed that the MT provide a "how to" in regard to communications and define a set of minimum equipment capabilities. The MT should avoid restating Treaty language and avoid restrictions on when and why the IT and the TS communicate; arrangements between the IT and ISP will establish what restrictions are needed. Where the MT currently refers to particular types of equipment (e.g. use of two-way radios) it would be better to outline basic standards for equipment rather than to set out specifications defined by specific technologies. The specific needs that MacLeod identified were communication needs in the field and between the BOO and the TS, voice between team members, overflight communications in the air and between air and ground, and the important needs of inspector morale (e.g. internet access, home calls, satellite television access).

Comments and Discussion

When asked whether communications between the teams on the ground and those in the air on an overflight is necessary, MacLeod noted that communications provides redundancy, which is needed for health and safety, and that it is needed just for carrying out the activities during the flight. A comment was made that such communications will need to be sure not to interfere with flight controls or operations. Another point made was that for continuation period techniques, it may be important to send data to the OSC for processing; MacLeod noted that such communications would be for data only. In response to those who might object to such data transfer, Shchukin noted that it may be in the best interest of the ISP to have off-site analysis of CPT data; many of the issues could be solved by resolving the communications issues. A question was asked about the case where the ISP provided the communications and whether this equipment had to be included in the CSP approved list of equipment; MacLeod suggested that this could be solved by developing minimal requirements, approved by States Parties.

Coxhead suggested that some parts of the MT need to be revisited; standards for communications need to be defined and the issue of equipment provided by the ISP need to be addressed. The functionality of communications equipment provided by the ISP should be the

same as that discussed here. The question is not so much what is needed in the manual, but rather what technical solutions are needed. In any case, parts of the manual may still need to be updated. Wang suggested that the discussion pointed to a need for a spectrum of documents: a paper defining equipment specifications, start up requirements, and basic objectives; a document outlining broad understandings for both parties; and documentation on technical and operational aspects in the form of SOPs supported by templates, logs, etc. The question of how many details to put in to these documents and how to be immune from future technical developments is an open question. Standards need to be present whether or not specific equipment becomes included in the approved equipment list. Difficulties could develop if specifications are made too fine and prevent use of future technical solutions.

Presentation: Balczo "Implementation of the Encryption Technology for OSI Purposes – Introduction"

In the final presentation of Session B, Balczo provided an overview of PTS activities in the area of preparing for secure communications during an OSI. He began by saying that what he would present was only initial work on the topic; the PTS needed much more experience and guidance on secure communications. He noted that secure communications involved technology, coupled with non-technical issues of confidentiality and the rights of the IT. Referring to paragraph 4.5.21 and Chapter 10 of the MT, he said that he thought that there was little need to encrypt voice communications from the field to the BOO and the MT should be modified in this area. He also referred to A3.1.14 through A3.1.16 of the MT, where encryption requirements were specified for the case when communications involved highly protected information. This also referred to some of the earlier discussions about confidentiality earlier in this workshop.

Balczo went on to discuss some initial systems that the PTS was investigating for dealing with encryption. The system being studied at the time was the Tiger XS personal encryption device for mobile and fixed communications (voice, data, fax, and secure messaging). He reviewed the technical details of secure voice, data, and fax transmission. This system was certified for European Union (EU) and North Atlantic Treaty Organization (NATO) standards for secret information; it employed a system administrator, a Tiger administrator, a cryptology custodian, and a system technician. The system did not work for all telephones. The PTS was still studying the system and new developments continued to occur. The system could also be used for land lines. He noted that, in order to use the system, PTS personnel would need to have vendor-required training for all elements (administrator, custodian, user) on how to use the system.

A prototype encryption system was technically tested on receipt by the PTS and used during DE10. It was easy to set up and reliable. Balczo noted that a lot of lessons were learned from DE10, such as how deep the PTS had to go into development to adapt the system for OSI use. In DE10 encryption was tried using various types of communication equipment. Communication from the field to the BOO worked fine, but communication from the BOO to headquarters in Vienna had some difficulties (related to the use of analogue lines). The source of most of the problems had been identified and could easily be solved. Many of these lessons learned will be incorporated into the establishment of the next version of the OSC.

Comments and Discussion

There were many questions about encryption keys, how they are handled and changed. Some of these issues were operational and some were system specific. Solutions would come by matching technology solutions with operational procedures. In response to a question, Balzco noted that effects on the efficiency of encrypted data transmission were not tested. He also noted that encryption currently was not part of the communications system. Additional discussion concerned the level of training needed for the systems and operational and maintenance requirements, which had important impacts on IT operations. When asked how ready the PTS was to give a proposal to WGB on encryption, Balzco answered that at the time the PTS was evaluating the exercise and that they would need to carry out a follow up procedure; thus they would not have a proposal ready for the next session of WGB in February 2010. Wang suggested that an update on progress at the next OSI workshop or during the August 2010 session of WGB might be appropriate. Finally, a participant suggested that information relative to the certification of an encryption system might be available from the EU or from NATO.

In summary, Wang suggested that there were several layers of issues concerning encryption:

- Policy guidance – there is not yet a consistent view on communications; particularly between the IT and headquarters.
- Technical issues –initial testing had been successful, but formal reporting is needed.
- Provider issues – the market for technology is not necessarily open.
- Procedural issues – the MT needs to be reviewed. What is the basic logic for communications and what needs to be shared with the ISP.
- SOPs still need to be developed.

Coxhead added several more issues for consideration:

- Do States Parties need to determine the levels of encryption needed?
- What is an adequate standard?
- The system described might work for communications between the IT and DG, but might not be suitable for regular use in the field – what is needed for regular communications?
- Should use of closed communication networks be considered?

Finally, he expressed the opinion that there is no need to define encryption standards in the OSI Operational Manual in any detail.

SESSION C: EQUIPMENT-RELATED PRE-INSPECTION ACTIVITIES

MacLeod, as subject leader for Session C, introduced the session with an overview of relevant material contained in the current MT. He noted that Section 3.9 had been modified as a result of discussions during the past few sessions of WGB and that there was an issue paper (IP_5) currently posted on the Expert Communication System (ECS). Finally, he emphasized the importance of equipment-related pre-inspection issues by noting that what was done in the pre-inspection phase and packed and shipped into the country would determine the success of the inspection.

Presentation: Arndt "Preparation of inspection equipment and related documents for the mandate"

Arndt provided two examples, based on PTS experience from IFE08, of types of equipment lists. The lists shown were lists of equipment in a container. He used these to show the need for guidance as to the level of detail that should be included. Should calibration history be attached? How should the TS document the fact that equipment is working?

Comments and Discussion

A participant commented that, to facilitate activities at the POE and equipment checking, documentation must be consistent. Reference should be made to the list approved by the CSP as well as the mandate, with a unique cross-reference identifier. Such cross-references and lists would also help to facilitate TS equipment selection by using records such as equipment use or maintenance history. Arndt noted that there was a plan to include reference documentation of the CSP approved list as well as use of sealed containers with sealed boxes. The history of the instrument would be part of a "subdocument" that included calibration data. Other recommendations were to have a picture of the equipment attached to the container, have TS personnel who were involved in equipment packing be part of the IT, and to use bar codes. Arndt noted that a bar code system was under development as a major project of the action plan for logistics along with the rapid deployment system. Coxhead noted that the distinction between core and auxiliary equipment was a good question and was a key to answering the question of what was meant by equipment checking. It would be important to find a middle level for documentation and cross checks that included all the needs for preparation, packing, shipping, and checking at the POE. One thought expressed was that core equipment could include items such as cables, and auxiliary equipment and would be things such as sleeping bags; but another opinion was that items such as cables could be used for different purposes and thus not be core equipment.

Presentation: MacLeod: "Pre-inspection activities"

MacLeod began his presentation by saying that most of his remarks were based on his experience with the Threshold Test Ban Treaty (TTBT), which from his perspective had a similar technical depth to the CTBT and similar issues with respect to equipment preparation and checking. He noted that discussion of Issue Paper 5 was open on the ECS and concerns Sections 3.3 and 3.5 of the MT. MacLeod stated that there were three categories of pre-inspection activities: 1) equipment selection; 2) equipment preparation; and 3) equipment documentation. Focus in this period should be on four key elements: 1) the level of ISP

logistics that would be provided; 2) lessons learned from previous use of the equipment; 3) equipment certification; and 4) equipment lists – the one for the mandate as well as the lists needed for shipping and packing. Standing arrangements were the key to the pre-inspection phase because they determined in a large sense what would need to be off-loaded at the point of entry (POE).

Delving into some of the details, MacLeod noted that it was important to maintain a history of how well a particular piece of core equipment worked; brand-new items, with no operational history, might not be the best. It helped to know how reliable the equipment was and how it fitted to a particular environment. Equipment with a history of problems should be relegated to training use or for spare parts. It was also important to have equipment spares. Exercises would help the TS to learn what particular needs would be in terms of equipment replacement and back-up. He noted that procedures were also needed for the period at the end of an inspection to decontaminate it and make sure it was ready for the next use. Naming and packing of equipment was an important consideration; division of equipment categories as auxiliary and core might not be sufficient and further subdivisions (e.g. administrative, initial period, continuation period, drilling) should be considered. Multiple types of lists need to be considered in preparing for an OSI: examples are container lists, the shipping manifest, inventory lists, certification lists, technical check lists, as well as the mandate list.

Referring to the MT, MacLeod suggested that a clearer distinction be made between certification seals and tamper indicating devices (TID), and that the MT contained a mixture of lists and purposes. For example, the mandate list needed to be as simple or "clean" as possible; currently there is a mixture of lists and purposes and no clear cross reference between the mandate and the list of equipment certified by the CSP. MacLeod closed his presentation with the following recommendations for the equipment list used for the inspection mandate:

- Use the equipment name as listed in the approved (CSP) list;
- Identify the inspection period when the equipment will be used;
- Include a reference code tied to the list of CSP approved equipment.

Comments and Discussion

In reference to the level of detail needed, a participant asked whether something like a hammer should be bar-coded. MacLeod replied that every piece contained in a toolbox did not need to be listed. There was also the issue of how to mark and certify such small pieces of equipment. When questioned about expendables, such as paper and printer cartridges, he suggested applying common sense; the mandate list was very general; the place where documentation was needed was for the case of information-gathering equipment -- the level of detail should be appropriate to the type of equipment. He also noted that a detailed list might actually expedite equipment checking – the level of detail might not be an issue for this, but it might be an issue for approval of the list approved by the CSP. Coxhead noted that at one level the list is for the mandate; at another level the purpose is transparency. Other comments were that legal procedures and facility agreements could help to facilitate checking and entry and that it could be useful to have a customs official present during certification, since equipment is present for examination at that time. Other comments referred to the need to pack the equipment intelligently with a mind as to when it would be needed and possible issues involved with software checking. A suggestion was made that software as part of a

particular piece of equipment should be part of the mandate. Prah noted that many of the issues under discussion were being addressed by the PTS; a current project projected use of 20-24 containers for an OSI.

Discussion also turned to the issue of medical supplies, including drugs or other controlled substances as well as special items like calibration sources for radiation measurement equipment. Coxhead suggested that there should be clear understanding between States Parties that such items have special understanding under this Treaty; the list of equipment should have some drugs and approved medical equipment that could be handled merely as part of the approved equipment list. There was also a need to define the different categories of things on the list; someone needs to do an analysis of what the separate things are – as an example for communications, the ISP would provide equipment, but the IT would have to have some of its own. There should also be modular concepts for various deployment strategies and different scenarios. A participant noted that such issues could be covered in concept of operations planning, with different plans for different scenarios. The plans could be minimal, but still have some level of detail according to environment and an associated equipment list. Walker noted that the OPCW has lists to the level of "first aid kit", for example, with details of the contents, and also has a list of allowed drugs.

In further discussion of software checking, MacLeod suggested one way would be to start up the equipment and check the software version, or to load software onto external media for checking, or to include software in the equipment familiarization. Another comment was that checking was not actually turning on equipment but merely checking seals at the POE. Arndt noted that software could have different functions and be subject to constant updates, so flexibility in checking is needed. He suggested that a special workshop might be needed to discuss software. MacLeod suggested that the TS would certify software in the equipment and put a tamper proof seal on equipment. The TS has to have the right software in a machine and the right software in the mandate; the question is at what level of detail the CSP would approve the software.

Additional discussion of software touched on making a distinction between machine software (e.g. operating systems) and analysis software, functionality of the equipment associated with the equipment (how complicated does it need to be) and software used for data collection. It might be possible to simplify some of the issues by using simpler technology, but this might not always be possible when using commercial products. One suggestion was that some questions of transparency might be dealt with via the equipment calibration process.

Coxhead introduced the issue of equipment spares; the serial number of the equipment and the possible need to check it against the mandate. He noted that in current concepts, the mandate is unchangeable, and all possible items of equipment must be listed, including replacements. One approach for allowing spares would be to make the mandate more general and not include serial numbers; this would allow spares and substitutions. He suggested that alternate ideas on how to deal with this issue in the mandate should be tested with a tabletop exercise.

SESSION D: OSI EQUIPMENT LIST

Shchukin, as subject leader for Session D, introduced the session by discussing the role of the equipment list in the Treaty from Part II, paragraphs 36, 37, 38, 50, and 51, of the Protocol – the list of OSI equipment approved by the CSP; core equipment and auxiliary equipment specified in Part II, paragraph 69 of the Protocol, and provisions for equipment certification, calibration, maintenance, etc., and the acceptance of approved equipment by the ISP on arrival of the IT. He noted that OSI Workshop-6 accomplished a great deal of initial work of creating the equipment list, with further later contributions and modifications. From time to time there is a need to modify specifications (e.g. ongoing modifications to still photography equipment which were also discussed at this workshop), but it is important to try to avoid making frequent changes. The general approach for the list to date has been to identify the type of equipment in conjunction with OSI activities and techniques, with primary functional requirements and technical specifications for the main components. Shchukin noted that some equipment (such as that needed for drilling) had not yet been considered by WGB and pointed out that there was still time to review the entire draft list of equipment. He provided a list of issues for discussion, which includes: how to include auxiliary equipment; how to deal with software, what is the level of detail needed, what is the experience from other treaties, and how WGB should proceed to a final version of the equipment list. In addition, he suggested that the group consider what identification information was sufficient to satisfy Part II, paragraph 51, of the Protocol (checking at the POE), and what information was needed for implementation of paragraph 38 (certification and seals).

Presentation: Arndt and Melamud: "Preparation of list of OSI equipment for approval by 1st conference of States Parties"

Arndt referred to the paragraphs in Part II of the Protocol regarding the list of equipment (paragraph 36), the first mention of auxiliary equipment (paragraph 37) and the provisions for maintenance, certification, and seals (paragraph 38). He proposed that the Organization for the Prevention of Chemical Weapons (OPCW) list of equipment be considered as a possible model for the OSI list. Some questions that need to be considered are which provisions are missing for OSI and which might not be needed. There are also questions about integrating calibration information into the list and whether there should be separate lists for core and auxiliary equipment. How should a balance be obtained between being too generic and too specific? Arndt used as an example a portable compressor unit that was used during the 2009 noble gas experiment (NG09) and tried to fit this equipment into a list similar to that used by the OPCW. His opinion from this exercise was that the OPCW list may be too generic. He presented a prototype table with suggested headings for the equipment list to be used to generate discussion. He noted that the equipment that had already been acquired for testing and training purposes (such as ground penetrating radar units) was developed as a result of the original work of OSI Workshop-6. The seismic aftershock measurement system (SAMS) was a good example of core equipment. He noted particular issues concerning software: for most off the shelf equipment, software went with the equipment; in addition there was processing software that was often needed. The IIMS would be the bridge between field equipment and software and the data processing software (e.g. such as is used for data collection and processing in the SAMS). He closed by suggesting some issues for discussion: formats for the tables of equipment lists; relevant procedures and text associated with each cell in the tables; and finding a definition of core and auxiliary equipment and software.

Comments and Discussion

In response to a question, Arndt indicated that the list could be sorted by subgroups. Other discussion concerned what types of information should be included in the list for approval by the CSP; one view was that certification and calibration information belong in the tracking and mandate lists, but this may also be problematic. The balance between generic and detailed information in the list is also important. Another participant noted that specifications for equipment should ensure no non-relevant use during an OSI and that distinctions should be made between "standard" use of the equipment versus uses specific to OSI. Shchukin suggested that it is time to begin work to "fill in the boxes" of the equipment list; for example the SAMS equipment list is ready for consideration by WGB soon. Again, opinion was expressed that calibration and certification columns are not needed in the CSP approval list; another person pointed out that the same arguments were considered in the OPCW and this type of information was not included. Shchukin suggested that the nature of the list for approval by the CSP was a good subject for an ECS discussion, which could also be geared towards what should be included on the database on equipment.

Presentation: Jia: "Consideration on the OSI equipment list"

Jia noted that the direct evidence of an underground nuclear explosion (UNE) is radioactivity and noble gases emanating from soil with radioactivity ratios conclusively supportive of an UNE, so radioactivity measurement equipment is a key element of an OSI. He presented a statistical approach for making a decision on radiation anomalies. In order to reduce the uncertainty of a decision, more samples would be needed, so more sets of equipment are needed. The selection of equipment should be based on evaluation of the effectiveness and applicability of equipment used in different scenarios. During development of inspection equipment, necessary software and hardware methods should be applied to ensure that the equipment can only collect information related to the purpose of the inspection, and post-processing methods should not be used to blind relevant information after measurement. The logistic support to inspection equipment should be simple and convenient to ensure successful conduct of an OSI.

Comments and Discussion

Some of the discussion focused on measurement restrictions for gamma measurements; the general suggestion was that these issues are an important way that technical solutions can be used to solve political questions. A participant also pointed out that issues such as measurement restrictions have to be included in the equipment list.

Presentation: Milbrath: "OSI Equipment list (with some focus on radionuclide/noble gas)"

Referring again to references to equipment in Treaty from Part II, paragraphs 36, 37, and 42, of the Protocol, Milbrath pointed out that not all equipment is brought on all inspections; the list does not specify what equipment would be used for a specific inspection; and the list does not deal with development priorities. He noted that during OSI Workshop-6 a table was developed of functional requirements and equipment specifications. He suggested a pathway towards developing an equipment list consisting of three steps: 1.) Develop the structure of

the list and the type of information needed; 2.) Select what equipment is to be on the list; and 3.) Determine the specifications of the equipment. He noted that both the PTS and States Parties should contribute by suggesting specific models of manufactured items as examples and that the list should be updated and amended as needed. In terms of level of detail, Milbrath suggested that naming specific makes and models of equipment should be avoided. He suggested that workshops or expert groups could provide a forum for development of the list, noting that, although not all technologies are ready for complete specifications; 85-90% of the equipment should be easily agreed upon. He provided an example of a possible structure for the list divided into categories of core and auxiliary equipment with the kind of information needed (in addition to technical specifications); a description and intended use (where it would be used); items grouped by how they are to be used (e.g. SAMS); and general operating requirements and specifications. Milbrath proposed that the list should be developed in parallel with a concept of operations and knowledge gained over time with development of the equipment should be continually incorporated. He followed up his structure description with an example drawn from radionuclide/noble gas equipment – soil gas measurements are a good example of the development of a concept of operations and equipment in tandem.

Comments and Discussion

A participant expressed agreement with the idea that the concept of operations works together with development of capabilities, and Milbrath pointed out that both do not have to be done at the same time. Another comment supported Milbrath's diagram of the equipment development cycle as a good technical approach and Milbrath noted that in the cycle, "ready for approval" meant the equipment was established and ready to remain in that status until entry into force (EIF) and the CSP-1. In response to a question, Milbrath agreed that functional requirements could be included in the development cycle; others reminded the group that specific restrictions and security aspects of equipment need to be included as well as part of the specification stage. Shchukin noted that the role of WGB would be approval once the initial specifications are developed and agreed upon. Other comments emphasized the importance of testing and exercises, training, and the method of work used during OSI Workshop-6 where expert groups were used to develop specifications. An important point was made comparing the OSI equipment list with the process of approval of station locations for the IMS – some stations had to be moved; but the general status is that of "…approval subject to final approval by CSP…". A similar approach could be made for OSI equipment to have some equipment ready ahead of EIF.

Presentation: Walker: "OPCW and approved equipment issues"

As a way of clarifying the experience of the Organisation for the Prohibition of Chemical Weapons, (OPCW), Walker provided a quick overview of how equipment lists were developed and handled in the Chemical Weapons Convention (CWC) and how they were presented to the First Conference of States Parties (CSP). He also discussed how changes to the list are handled, how equipment familiarization is done, and how the equipment is presented in inspection mandates. In Walker's opinion, all of this provides lessons for CTBT/OSI. Walker noted that the OPCW list includes specific operational requirements, technical specifications, and common evaluation criteria (e.g. air transport, drop tests, etc.). Health and safety equipment is included (the suggested medical kit is left to the physician) and there are a total of 22 separate cross-referenced documents that comprise the technical specifications. Walker showed a specific example of a list and suggested that participants

refer to the OPCW web site where a copy of the First Conference of States Parties Decision on approved equipment can be found at http://www.opcw.org/documents-reports/conference-states-parties/first-session/, which has a table with references. Some of the categories of equipment used by the OPCW are "portable", "protective and safety", "medical", "administrative", and "occupational health" items. As an example of operational requirements used by the OPCW, Walker showed those for a gas chromatograph/mass spectrometer, which had relatively general descriptors. He used health and safety equipment as an example of general requirements.

With respect to amendments and changes to the OPCW list, Walker noted that the OPCW can change requirements as a result of field experience; when a change is put to the CSP, certain justifications and requirements, along with alternative benefits are generally cited. Notification of changes are worked through the DG and a new familiarization process takes place. Familiarization is done "…sufficiently prior to its use on the territory…". An approved mandate format is used for regular challenge inspections; the States Parties would already have the technical details of the equipment, so they would only need to refer to the name of equipment. Walker provided an example of an equipment list used for an inspection. In his conclusion, Walker suggested that the OPCW is a good model for what is done in OSI as it addresses comparable concerns in the CTBT context – confidentiality, security, safety, and technical specification details..Its regime also offers the States Parties opportunities to familiarise themselves thoroughly with inspection equipment at the OPCW well before it is brought on any inspection.

Comments and Discussion

In response to a question, Walker said that he was not aware of a provision in the Chemical Weapons Convention (CWC) itself that a State Party could insist that specific commercial equipment models should be used. A participant asked that since items listed are relatively generically described and familiarization is for a specific model how does a State Party satisfy that this fulfills requirements? Shchukin suggested that with the current double loop PTS procurement process, a State Party could revise specifications during the preliminary part of the loop. One difference between the OPCW and the CTBT that was noted is that the CTBT does not anticipate changes in the list of equipment; perhaps consideration should be made in the CSP to allow for equipment changes. Walker noted that for the OPCW, the hard work on equipment was done before the CSP; there was no debate on the floor during the Conference.

SESSION E: PREPARATION FOR THE NEXT IFE

Prah, as subject leader for Session E, introduced the topic by noting that an IFE is an element of the OSI Revised Strategic Plan (INF.793) – it is part of the development and testing cycles foreseen in Phase 1 of that plan. The second cycle of Phase 1 started with the action plan (INF.1020) adopted by the PrepCom last year. Rozhkov, Director of the OSI Division, presented the draft document describing preparations for the next IFE.

Presentation: Rozhkov "Planning concept in preparation for and conduct of the next IFE"

Rozhkov began by noting that a document titled "PTS Planning Concept in Preparation for and Conduct of the next Integrated Field Exercise (IFE)" had been posted on the ECS for comment. He emphasized that the purpose of integrated field exercises was to build up OSI capability. The PTS would use the time leading up to the next exercise to plan and exercise essential OSI elements and assess them for capabilities. The current plan represented a best effort of the PTS to offer for WGB consideration. The intent was to provide a mechanism to develop OSI operational capability in incremental blocks as follows:

1. Launch phase – from receipt of OSI request through launch to arrival at POE.
2. Pre-inspection phase – from arrival at POE to establishing BOO.
3. Inspection phase – actual inspection activities.
4. Post-inspection phase – from the end of the inspection through report preparation to IT recovery.

Rozhkov noted that items 2 and 4 would be done together in one separate exercise. The launch phase block would be done as a command post exercise (with role playing) in early 2012; be of 5 days duration, and include 40 participants. The pre- and post-inspection phases blocks would be done as a field exercise during the third quarter of 2012; be of 7 days duration, and include 60 people. The third block would consist of a 10-day field exercise in 2013 that will test newly developed core-critical technologies. This exercise would take place near Vienna or in a neighbouring country. There would be a number of expert meetings prior to these exercises for planning, and Rozhkov stressed that well-trained participants (relying on the advanced training programme) would be needed for this. The full IFE is planned for the second half of 2014.

Rozhkov noted that a project management approach will be used, with one overall project team in charge of development. The PTS intends to use task force groups for IFE planning, with heavy reliance upon experts from States Signatories or some kind of expert adviser mechanism. He said that at least one year would be needed for focused preparation for the IFE. The document posted on the ECS contained a listing of the technologies that would be exercised during the IFE. Most important, Rozhkov emphasized, is the need for a detailed, realistic, scientifically and technically credible scenario. He noted some critical dependencies that include: implementation of action plan projects; availability of infrastructure and support mechanisms (e.g. ESMF, OSC, training -- both surrogate inspectors and PTS personnel – IDC, IMS, administrators); availability of human resources (the estimate was that 30 people from the PTS would be needed); and availability of appropriate budget. He provided estimates of additional costs, in excess of the current budget, that would be needed for proper

development of the project. Rozhkov closed by requesting the support of States Signatories in the form of contribution of experts, long term in-kind equipment contributions (especially for radionuclide/noble gas equipment, sampling, multispectral infrared equipment, and CPT equipment), help on the design and script of the IFE, provision of local nearby exercise areas for build-up, and finally a host for the IFE venue.

Comments and Discussion

In the discussion, Rozhkov stated that the IFE would start with all equipment and shipment pre-planned and initial preparation already complete. He noted that this was for financial reasons; the intent of the exercise was, inter alia, to test OSI data collection capabilities, such as noble gas collection, and financial resources would be allocated accordingly. He also pointed out that the plan gives leeway to States Signatories as to the budget considerations (in terms of approving the requested budget increases in the plan). One participant commented that the focus on a scientifically credible scenario is very important, noble gas sampling and analysis should be a core objective, and that the PTS should be sure to refer to the lessons learned database. Rozhkov noted that the lessons learned database was incorporated into the current PTS action plan and that management of the exercise would be done by a project management team that was aware of the need to find proper balance of activities to test versus budget restraints and the state of equipment development. A participant pointed out that many of the preparation activities would still need to be done whether or not the IFE exercise and budget approvals were made by WGB. Rozhkov also noted that there is an issue of human resources in the PTS; the PTS has made estimates of the impact of these on time and money and connections with training. Additional comments were that the IFE should be managed as an exercise, not an event, and that management of outside resources should be considered in the planning process with advanced notice to States Signatories if more resources are needed. In summary, Prah noted that all had taken a positive approach to the planning document and it would be put on the ECS for discussion. Comments from this workshop would be taken into account when modifications were made later in December.

FINDINGS AND RECOMMENDATIONS

SESSION A: INSPECTION TEAM DATA HANDLING AND CONFIDENTIALITY

- The PTS is recommended to carry out a study to determine the data needed prior to an inspection that needs to be compiled by the TS for an IT. (Note that further consideration will be needed on the sources of such data.)

- Clear technical measures are needed to protect data gathered in the IA (consistent with an overarching policy framework for the TS), including:

    - Archival copying of original data,
    - Appropriate protection measures for IT communications, including encryption,
    - Measures to prevent unauthorized access to data,
    - Measures to purge data from inspection equipment at the end of an inspection.

- The current PTS development work on the IIMS is welcomed. This data management tool should help to provide information protection, taking into account lessons from IFE08 and the following considerations:

    - Adjustments may be needed in the MT to accommodate new arrangements, including considerations of the proposal for a "receiving area".
    - The IIMS should provide flexibility for different types of data, such as where and how samples have been taken.
    - Questions were raised about handling of data judged to be non-relevant, or for which the classification level is altered after entry into the IIMS. Data purging at the end of the inspection, when needed, should provide assurance to the ISP that such information is secure.
    - Questions were raised about the practicality of some provisions in the draft OSI Operational Manual requiring joint storage of particular types of data, such as the case when data is held in centralized storage, such as groups of hard drives.

- With respect to the handling of sensitive information and data by the IT, consideration is needed on the pros and cons of a multi-level or single-level protection arrangements, including the following:

    - Advantages of separating need-to-know criteria from classification arrangements,
    - Advantages or disadvantages of a possible alternative data protection framework based on the idea of a single classification level,
    - Utility of a tabletop exercise to test some of these issues,
    - Necessity of special data protection arrangements for some techniques such as how CPT should be handled.

- Further consideration could be given to whether the approach taken by the IAEA to

the classification of sensitive information can offer lessons for CTBT OSI.

SESSION B: INSPECTION TEAM COMMUNICATIONS

- There is need to establish minimum standards for IT communication requirements. Such requirements need to cover most foreseeable scenarios and provide for redundancy. Recent progress by the PTS in this regard is recognized.
- At the beginning of its inspection mission, the IT assumes self-reliance and sufficiency for provision of communication equipment. Such provisions are subject to operational arrangements with the ISP, including the allocation of frequencies and VSAT license.
- The TS and IT need to remain open to the use of ISP-provided communication means and equipment, as far as the provided sets meet the IT requirement standards. The ISP is expected to allocate specific frequencies to correspond to its equipment for IT use.
- The IT has the right to communicate with the TS at any time and under the coverage of the Vienna Convention on Diplomatic Relations (VCDR).
- The PTS is recommended to provide draft proposals for communication equipment requirements and specifications based on their recent market search and field testing and to continue preparations of concepts of operations for communication and SOPs.

Several pending issues were recognized:

- The level of documentation to provide policy guidance for the TS and IT and to ensure that a State Party undertakes efforts to ensure communications support needs to be determined.
- Determination needs to be made concerning whether transmission of inspection data from the IA by the IT to the TS for processing should be allowed.
- Textual inconsistencies in the MT that may be counter to provisions of the Treaty need to be reviewed.

Encryption Issues

- Encryption of telecommunications equipment is required for the IT to communicate in private with the TS. When communications equipment is provided by the TS, the encryption device and key will be held by the TS and IT. For communications equipment provided by the ISP, the encryption device and key will be held by the ISP.
- The PTS has conducted an informative market search and field testing during DE10 of encryption options to secure voice, data, fax and SMS communications via various networks, satellite systems and landlines. Such efforts should continue so that the PTS may be ready to propose solution options as early as 2011.
- The concept of operations and SOPs for encryption need to be developed.

Pending Issues for Encryption:

- Consensus is yet to be achieved on the policy issue of whether the ISP may obtain, retain, or share an encryption key for IT communications with the TS. (Whether the encryption key that is provided by the ISP needs to be in duplicate -- with one for the TS/HQ -- remains to be solved.)
- There is no agreement yet whether the in-field IT communication or transmission of data would need encryption.
- Current provisions of the MT concerning encryption should be reviewed. Certain provisions give rise to different interpretations and some may be difficult to implement, such as those contained in sections A3.1.14, 15, and 16.

Recommendation

The PTS should conduct a short technical workshop/short field exercise to test MT and SOPs on digital photography to include testing of cameras, forensic trail, confidentiality review process from point of collection, review and reporting aspects, or do so as key part of the IFE 14 exercise programme. (And in the IFE Concept Implementation, the proposed field exercise for autumn 2012, which is to include exercising basic field skills.)

SESSION C: EQUIPMENT-RELATED PRE-INSPECTION ACTIVITIES

- Equipment selection is based on the mandate and is an integral part of initial planning for the inspection.
- ISP logistics support drives equipment needs and team composition.
- The MT should be reviewed to address the following:
    - What is core and auxiliary equipment,
    - What is the difference between core and auxiliary equipment,
    - Additional category breakdowns may be need for improved clarity,
    - The status of software as core or auxiliary needs to be determined.
- A unique identifier from the Conference of States Party approved equipment list should be a common reference for all lists used for the equipment.
- Equipment should be certified at the “tool box” level based upon the CSP approved list and not at the “screwdriver” level, and listed as such in the mandate with the number of pieces.
- Certification lists and the mandate list should include the model and serial number of each item of equipment.
- Distinction should be made between certification and tamper indicator device seals with clear distinctions about how these indicators are used.
- The MT should be reviewed to address the following:

- Procedures to ensure calibration, maintenance of the equipment for certification, and use history are tracked.
- Equipment with a history of frequent problems when used for OSI should not be used.
- Training sets of equipment should be distinct from the deployment set.
- Procedures are needed to ensure that equipment has been purged and decontaminated.

- SOPs are needed for the following:
  - Equipment labelling, box labelling, the inventory list, container labelling, ensuring ease of inventory and POE inspection, and tracking activities and equipment location during use;
  - Inclusion of medical equipment and controlled substances such as narcotics, which need special handling.
- More discussion on familiarization and software control is needed for:
  - Provisions for software to be loaded on the equipment instead of being in external storage and loaded at the BOO;
  - Dealing with the concept of data acquisition software as distinct from data analysis software.

SESSION D: OSI EQUIPMENT LIST

- The equipment list is important both for facilitating availability of appropriate OSI equipment and for assuring its prompt entrance into the territory of the ISP.
- There is a need for systematic work on further development of the list, particularly on the structure of the list as well as for identification and refinement of specifications of equipment to be used for OSI and development of concepts for use of this equipment. All States Signatories are encouraged to participate actively in this work.
- Approaches suggested in the presentations based on the OPCW list of equipment could be a good starting point for further development of a template for the OSI list of equipment.
- The OSI equipment database could be a useful tool for getting a full detailed description of the OSI equipment. The PTS is encouraged to accelerate development of such a database as well as an overall equipment-related documentation management system. All States Signatories are encouraged to participate actively in the development of the OSI database.
- It is recommended that the general structure and content of the list as to core equipment be tailored to inspection activities and techniques as described in Part II, paragraph 69, of the Protocol.
- Functional/operational requirements and specifications of equipment in the list should reflect, as appropriate, limitations related to protection of sensitive information and

preventing collection and retention of such information not related to the purpose of OSI.

- OSI Workshops incorporating concerted use of expert groups to develop the equipment list and specifications, in an approach similar to OSI Workshop-6, are deemed to be an effective element of the entire mechanism of development of the list.

Continuing Issues

- The need to include calibration requirements in the equipment list should be further evaluated.
- Guidelines for revision and update of the list need to be developed, taking into consideration the OPCW approach.
- There is a need to define necessary information to be included in the list of approved OSI equipment.
- Further definition of auxiliary equipment is needed.

SESSION E: PREPARATION FOR THE NEXT IFE

Refer to the document "PTS Planning Concept in Preparation for and Conduct of the next Integrated Field Exercise (IFE)" as posted on the ECS on 25 November, 2010.

As requested at the 35th session of WGB, a draft concept for building OSI operational capability through a series of exercises prior to undertaking the next IFE has been prepared and as part of the consultation process has been presented at Workshop-18 under Session E: Preparation for the next IFE. This concept is developed to assist States Signatories in identifying the scope, components and appropriate time allocation for the next IFE. The main objectives of the draft concept are to:

- Establish an exercise mechanism, developed as a result of implementing the OSI action plan.
- Put in place a flexible exercise approach that enables a dynamic build up and steady accretion of OSI capabilities, in particular with a focus on core/critical capabilities development.
- Maximize cost efficiencies through the use of local exercise areas whenever feasible; and seek for synergies among the different OSI activities such as the conduct of the second training cycle for surrogate inspectors.

The main outcomes from the discussion are:

- The draft concept is encouraging and represents a very good basis for activities that will lead to implementation and conduct of the next IFE.
- Noble gas collection and analysis was identified as one of the key priorities that should be exercised in the next IFE, as rightly identified in the concept.

- An integrated evaluation that covers the entire build-up process for the next IFE needs to be put in place as reflected in the concept paper.
- Lessons learned from previous OSI events and especially from the IFE08 should be taken into account for the planning and preparation of the next IFE.
- The need for a detailed, realistic and scientifically credible scenario has been highlighted in the discussions.
- The OSI action plan, as endorsed by the PrepCom, is very important and needs to be implemented even if it is not possible to conduct an IFE in 2014.
- The necessity to exercise available OSI elements has been reiterated; the next IFE should focus on those aspects of the OSI regime that are difficult to evaluate in smaller targeted activities and should emphasize the required synergies that can only be tested and demonstrated in an IFE.
- More details and justifications on the financial and human resources requirements for implementing the proposed draft concept have been requested, including the concept of PTS wide involvement in planning, preparation, conduct and evaluation of an IFE.

Acknowledgements by the Rapporteur

The Rapporteur would like to thank the workshop chairpersons and the subject leaders for guiding the development and discussion of the findings and recommendations, which are the most important part of this report. I also thank the OSI Division Documentation Section, especially Deng Hongmei and Marie Tweed, for their very professional and efficient support in assisting with the development of this document. Finally, I thank the many participants of the workshop who provided their comments on the drafts of this report.

ANNEX I

LIST OF PRESENTATIONS

Opening Session

1. Rozhkov, O., PTS, Opening remarks.
2. Shchukin, V., Russian Federation, Objectives of Workshop-18 (CTBT/OSI/WS-18/PR/18).
3. Coxhead, M., Australia, Focus on the draft OSI Operational Manual - Introductory comments by the Task Leader (CTBT/OSI/WS-18/PR/13).
4. Sweeney, J., USA, Guidance on workshop report drafting.
5. DENG Hongmei, PTS, Administrative information.

Session A: IT Data Handling and Confidentiality (& Handling of Digital Images)

6. Coxhead, M., Australia, Introductory comments on IT data handling and confidentiality (CTBT/OSI/WS-18/PR/14).
7. Balczo, B., PTS, OSI data handling and confidentiality in the field and at the OSC.
8. Labak, P. PTS, Integrated Information Management System (IIMS) and data handling during an OSI (CTBT/OSI/WS-18/PR/15).
9. Ciganikova, D., PTS, Data handling during the pre-inspection period (CTBT/OSI/WS-18/PR/17).
10. MacLeod, G., USA, OSI confidentiality considerations (CTBT/OSI/WS-18/PR/03).
11. HAN Xiaoyuan, China, Consideration on IT data handling and confidentiality (CTBT/OSI/WS-18/PR/02).
12. Osugi, S., Confidential issues for CTBT (CTBT/OSI/WS-18/PR/06).
13. Walker, J., Brief introduction (CTBT/OSI/WS-18/PR/01).
14. Kaltseis, C., Austria, Handling of digital images and experience from forensic works (CTBT/OSI/WS-18/PR/19).

Session B: IT Communications

15. Wang, Jun, China, Brief introduction (CTBT/OSI/WS-18/PR/04).
16. Prah, M., and Abushady, A., Communication testing during DE10 (CTBT/OSI/WS-18/PR/12).
17. MacLeod, G., Sweeney, J., and Arzigian, J., USA, OSI communications (CTBT/OSI/WS-18/PR/05).
18. Balczo, B., Implementation of encryption technology for OSI purposes – Introduction (CTBT/OSI/WS-18/PR/16).

Session C: Equipment Related Pre-Inspection Activities

19. Arndt, R., PTS, IFE08 equipment packing templates (CTBT/OSI/WS-18/PR/20).
20. MacLeod, G., and Sweeney, J., USA, Pre-inspection activities (CTBT/OSI/WS-18/PR/07).

Session D: OSI Equipment List

21. Shchukin, V., Russian Federation, Development of the list of OSI equipment (CTBT/OSI/WS-18/PR/21).
22. Arndt, R., and Melamud, M., PTS, Preparation of the list of OSI equipment for approval by the first Conference of States Parties (CTBT/OSI/WS-18/PR/08).
23. JIA Mingyan, China, Consideration on the OSI equipment list (CTBT/OSI/WS-18/PR/09).
24. Milbrath, B., USA, OSI equipment list (with some focus on radionuclide/noble gas) (CTBT/OSI/WS-18/PR/10).
25. Walker, J., UK, OPCW and approved equipment issues (CTBT/OSI/WS-18/PR/11).

Session E: Preparation for the Next IFE

26. Rozhkov, O., PTS, Planning concept in preparation for and conduct of the next IFE.

ANNEX II

SUGGESTION PAPER PROVIDED BY THE TASK LEADER FOR THE DRAFT OSI OPERATIONAL MANUAL FOR SESSION A

Suggestion for alternative data protection arrangements

1. Data handling and protection arrangements applied by the IT and ISP in the field and the BOO will be based on a single set of procedures that are designed to maximise data protection while maintaining inspection effectiveness, including:

- data is recorded systematically using predefined mechanisms
- where practicable, an archival read-only copy of data is retained under joint control
- data access is based on need-to-know as defined below
- all data access is logged automatically
- systems are designed to prevent unauthorised disclosure (by insider or by external monitoring)
- encryption will be applied for all data transmission and storage within the IT (transmission outside is a separate issue).
- IT LAN is physically isolated
- measures will be applied to avoid undetected tampering with data after it is recorded in the field, and before it is entered into the IIMS.

2. Classification arrangements remain, but are applied where data or information is passed to third parties. Thus, IT reports would be subject to classification by the ISP when issued. (Minimum level for reports is OSI Limited. IT could choose higher classification if ISP does not.)

3. Need-to-know (NTK) guidance is not based on data classification. The ITL decides on NTK for each team member, which normally would give the team member access to all data relevant to his/her functions, plus access to results of other inspection activities (to enable synergies).

4. The ISP may, as part of managed access negotiations, or as a condition for providing some data directly to the IT, specify that access to certain data will be limited to small number of team members. The ITL will negotiate with the ISP on such arrangements. Data subject to such arrangements could remain outside the FIMS, and probably in joint storage.

If local confidentiality regulations require, additional security arrangements could be negotiated, but these should not be applied so as to limit inspection effectiveness.

5. The above-mentioned data handling arrangements would be implemented through the IIMS in as user-friendly a way as is possible. As data storage for the IIMS is centralised, the idea that specific data is held in joint storage when not in use becomes harder to implement.

6. Centralised data storage, and routine use of electronic systems also makes it more difficult to demonstrate to the ISP that data has been deleted (for example) if found not to be relevant. Can we understand that return to the ISP can only be proven at the end of the inspection when equipment is purged of data (or destroyed)?

7. If a single level of protections is applied, there may not be any indicators to IT members on the relative sensitivity of inspection information. So, if, for example, in field communications are not fully secure, will general guidance (e.g. avoid discussing inspection findings) be enough?

ANNEX III

LIST OF REFERENCE MATERIALS

OSI manual provisions in the Model Text (CTBT/WGB/TL-18/40) and Annotated Draft Rolling Text (ADRT, CTBT/WGB/TL-18/27) most relevant to workshop topics

Session A: IT data handling and confidentiality

- Section 5.4 on delineation of the BOO into different parts for the application of privileges and immunities.
- Paragraphs 10.4.12 to 16 on arrangements for classification of information gathered in the IA.
- Paragraph 10.4.20 on application of the need-to-know principle.
- Annex 3.1 on data protection procedures.
- Various provisions (e.g. 4.3.10, 6.3.57-57, 6.7.3(d), 6.8.14, 10.4.24) on custody and handling of data, and para 6.2.60 on Analysis/Integration of Initial Overflight Data.

Session A: IT data handling and confidentiality --- handling of digital images

- Section 6.7 on still and video photography
- Para 4.3.13(iii) on structure of the BOO
- Para 6.2.60 on Analysis/Integration of Initial Overflight Data

Session B: IT communications

- Section 4.5 on communications, especially 4.5.9
- Annex 2.2 – which needs to be replaced with something suitable for the requirements of 4.5.9
- Annex 3.1, paragraphs 14 to 17 in relation to encryption of electronic data transmission

Session C: Equipment-related pre-inspection activities

- Section 3.9 on selection and preparation of inspection equipment
- Para 3.12.15 on identification of equipment in the mandate
- 4.1.28-29 on equipment checking by ISP
- Relevant deployment strategies, equipment preparation for shipping and associated paperwork

Session D: OSI Equipment List

- ADRT, part G, Annex 6.1- 6.4

Session E: Preparation for the next IFE

- None

ANNEX IV

LIST OF PARTICIPANTS

ARMENIA

Mr Hayk HAKOBYAN
Armenian National Survey for Seismic Protection
Davidashen 4 massiv
0054 Yerevan
Tel.: +37410286494; +37491862134
Fax: +37410282811
Email: *alinakop1948@mail.ru; alinakop2004@yahoo.com*

AUSTRALIA

Mr Malcolm COXHEAD
ASNO, RG Casey Building
John McEwen Crescent
Barton, ACT, 0221
Tel.: +61262611913
Fax: +61262611908
Email: *malcolm.coxhead@dfat.gov.au*

AUSTRIA

Mr Christoph KALTSEIS
Am Kematnerberg Nr. 2
4531 Kematen/Krems
Tel.: +43 699 1233 3400
Email: *office@lightstorm.at*

CHINA

Mr HAN Xiaoyuan
Northwest Institute of Nuclear Technology (NINT)
28 Pingyu Road, Baqiao District
Xi'an 710024
Tel.: +86 29 847 65141
Fax: +86 29 833 66333
Email: *hxytm@sina.cn*

Mr JIA Mingyan
Northwest Institute of Nuclear Technology (NINT)
28 Pingyu Road, Baqiao District
Xi'an 710024
Tel.: +86 29 847 65141
Fax: +86 29 833 66333
Email: *huaxiuwang@163.com*

Mr LIANG Guotao
Permanent Mission of China
Geroldgasse 7
1170 Vienna, Austria
Tel.: +43 1 486 1635
Fax: +43 1 484 1633
Email: *liang_guotao@mfa.gov.cn*

Mr MA Shengkun
Permanent Mission of China
Geroldgasse 7
1170 Vienna, Austria
Tel.: +43 1 486 1635
Fax: +43 1 484 1633
Email: *ma_shengkun@mfa.gov.cn*

Mr WANG Jun
Ministry of Foreign Affairs
Chaoyangmen Nandajie No. 2
100701 Beijing
Tel.: +13439718616
Email: *wang_jun3@mfa.gov.cn*

CROATIA

Mr Boris ILIJAS
State Office for Nuclear Safety
Ulica Grada Vukovara 284
10000 Zagreb
Tel.: +38599314965
Fax: +38514830109
Email: *boris.ilijas@dzns.hr*

FINLAND

Mr Pasi LINDBLOM
Institute of Seismology
Gustaf Hallstromin katu 2b
00014 University of Helsinki
Tel.: +358 50 3301662
Fax: + 358 9 19151598
Email: *pasi.lindblom@helsinki.fi*

FRANCE

Mr Benoit DUCHENET
Permanent Mission of France
Schwarzenbergplatz 16
1010 Vienna, Austria
Tel.: +43 1 501 82 334
Fax: +43 1 501 82 339
Email: *benoit.duchenet@diplomatie.gouv.fr*

Mr Axel HEYSER
Unité Francaise de Vérification
UFV BA 110
60314 Creil
Tel.: +33 344287154
Fax: +33 344286290
Email: *axel.heyser@free.fr*

GERMANY

Mr Franz GRONESCHILD
Bundeswehr Arms Control Verification Center
Quimperle Strasse 100
52511 Geilenkirchen
Tel.: +49 2451-992285
Email: *franzgroneschild@bundeswehr.org*

HUNGARY

Mr István TÖRÖK
Eötvös Loránd Geophysical Institute of Hungary
Columbus Str. 17-23
1145 Budapest
Tel.: +36 1 2524999
Fax: +36 1 3637256
Email: *torok@elgi.hu*

IRAN (ISLAMIC REPUBLIC OF)

Mr Mehdi ALIABADI
Permanent Mission of the Islamic Republic of Iran in Vienna
Jauresgasse 3
1030 Vienna, Austria
Mob. +43 699 1082 2420
Tel.: +43 1 26 99 660
Fax: +43 1 26 99 791
Email: *aliabadi_me@yahoo.com*

Mr Mahdi BOUSTANI
Shahid Beheshti University
Evin St.
Teheran
Tel.: +98 21 29902541
Email: *m_golestani47@yahoo.com*

Mr Mahdi GHOLAMI
Ministry of Foreign Affairs
Building No.8, 30 Tir St.
Teheran
Tel.: +98 21 61154438
Fax: +98 21 61154513

Mr Seyed Mehdi HOSSEINI ESFIDVAJANI
Permanent Mission of the Islamic Republic of Iran in Vienna
Jauresgasse 3
1030 Vienna, Austria
Tel.: +43 699 10822420
Fax: +43 1 2699791
Email: *hosseini_sme@yahoo.com*

Mr Mohammad SABZIAN
Ministry of Foreign Affairs
Building N0.8 west, 30 Tir St.
Teheran
Tel.: +98 2161154438
Fax: +98 2161154513
Email: *sawyer.taylor@hotmail.com*

Mr Mohammad Hassan ZAHMATKESH
Shahid Beheshti University
Evin St.
Teheran
Tel.: +98 21 29902541
Email: *mheair@yahoo.com*

JAPAN

Mr Shigeru OSUGI
Center for the Promotion of Disarmament and Non-Proliferation (CPDNP)
3-2-5 Kasumigaseki
100-6011Chiyoda-ku, Tokyo
Tel.: +81335037558
Fax: +81335037559
Email: *shigeru.osugi@cpdnp.jp*

RUSSIAN FEDERATION

Mr Vadim PROSTAKOV
State Atomic Energy Corporation "Rosatom"
Bolshaya Ordynka Str. 24 Bld.
119017 Moscow
Tel.: +7 499949-4174
Fax: +7 499949-4068
Email: *VIProstakov@rosatom.ru*

Mr Vitaly SHCHUKIN
Russian Federal Nuclear Centre
Tsiolkovsky street 8-10
Snezhinsk 456770
Chelyabinsk Region
Tel.: +73514654105; +73514654730; Mob. +79226374038
Fax: +7 35146 55118
Email: *osi_coordinator@hotmail.com; v.n.shchukin@vniitf.ru*

Ms Emiliya SIDOROVA
Permanent Mission of the Russian Federation to the International Organisations
Erzherzog Karl Str. 182
1220 Vienna, Austria
Tel.: +43 1 2825391
Email: *Rfmission-vienna@chello.at*

SLOVAKIA

Mr Milan TICHY
Nuclear Regulatory Authority Department for international relations and EU matters
Bajkalská 27
00421/82007 Bratislava
Tel.: +421258221157
Fax: +421258221166
Email: *Milan.Tichy@ujd.gov.sk*

SRI LANKA

Mr Athula Theja Bandara MUDUNKOTUWA
Geological Survey & Mines Bureau
Senanayake Building No. 4, Galle Road
Dehiwala
Tel.: +94112725745
Fax: +94112735752
Email: *mudunkotuwa@gsmb.gov.lk; athula_mudunkotuwa@yahoo.com*

UK

Mr John WALKER
Arms Control and Disarmament Research Unit
Foreign and Commonwealth Office
King Charles Street
London SW1A 2AL
Tel.: +44 20 7008 2255
Fax: +44 20 7008 2860
Email: *john.r.walker@fco.gov.uk*

Mr Jonny HARTNELL
Atomic Weapons Establishment AWE
Aldermaston, Reading
Berkshire RG7 4PR
Tel.: +44 11 8985 6038
Email: *jonny.hartnell@awe.co.uk*

UNITED STATES OF AMERICA

Mr James ARZIGIAN
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1374
Tel.: +1 505 844 2747
Fax: +1 505 844 8119
Email: *jsarzig@sandia.gov*

Mr John GODFREY
U.S. Department of State
Wagramer Strasse 17
1220 Vienna, Austria
Tel.: +43 664 9670 101
Fax: +43 1 3133 94795
Email: *GodfreyJT@state.gov*

Mr Todd KONKEL
U.S. Department of State
Wagramer Strasse 17
1220 Vienna, Austria
Tel.: +43 664 8334 009
Fax: +43 1 313394795
Email: *KonkelTR@state.gov*

Mr Gordon MACLEOD
JNPO/Los Alamos National Laboratory
232 Energy Way MS NSF163
North Las Vegas, NV 89030
Tel.: +1 702 2952927
Fax: +1 702 2951269
Email: *macleod@lanl.gov*

Mr Brian MILBRATH
Pacific Northwest National Laboratory
902 Battelle Blvd.
Richland, WA 99352
Tel.: +1 509 3765368
Fax: +1 509 3765824
Email: *brian.milbrath@pnl.gov*

Mr Michael NEWMAN
U.S. Department of Energy/
National Nuclear Security Administration
Office of Nuclear Verification
1000 Independence Avenue, SW
Washington, DC 20585
Tel.: +1 202 586 2245
Fax: +1 202 586 6789
Email: *mike.newman@nnsa.doe.gov*

Mr Nhan NGUYEN
Permanent Mission of the United States of America to the CTBTO
Wagramer Strasse 17-19
37th Floor, IZD Tower
1220 Vienna, Austria
Tel.: +43 1 31339 4725
Fax: +43 1 31339 9725
Email: *nguyennt@state.gov*

Mr Gilbert SATEIA
U.S. Department of State
2201 C Street N.W., Room 5669
Washington, D.C. 20520
Tel.: +1 202 647 8685
Fax: +1 202 736 7634
Email: *sateiagi@state.gov*

Mr Jerry SWEENEY
Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550
Tel.: +1 925 422 4917
Fax: +1 925 423 4077
Email: *sweeney3@llnl.gov*

CTBTO Preparatory Commission
Provisional Technical Secretariat

Vienna International Centre
P.O. Box 1200
1400 Vienna, Austria

On-Site Inspection Division

Office of the Director

Mr Oleg ROZHKOV
Director
Tel.: +43 1 26030 6201
Email: *oleg.rozhkov@ctbto.org*

Mr Matjaz PRAH
Coordinator
Tel.: +43 1 26030 6399
Email: *matjaz.prah@ctbto.org*

Policy Planning and Operations Unit

Mr Ashraf ABUSHADY
FIMS and Communications Officer
Tel.: +43 1 26030 6284
Email: *ashraf.abushady@ctbto.org*

Mr Luis GAYA-PIQUE
Policy Planning Officer
Tel.: +43 1 26030 6429
Email: *luis.gaya@ctbto.org*

Mr Alex LAMPALZER
Policy Planning Officer
Tel.: +43 1 26030 6518
Email: *hermann.lampalzer@ctbto.org*

Ms Ditta CIGANIKOVA
Operations Officer
Tel.: +43 1 26030 6393
Email: *ditta.ciganikova@ctbto.org*

Documentation Section

Ms DENG Hongmei
Chief
Tel.: +43 1 26030 6172
Email: *hongmei.deng@ctbto.org*

Ms Marie TWEED
Documentation Officer
Tel.: +43 1 26030 6474
Email: *marie.tweed@ctbto.org*

Mr Kevin STICKNEY
Documentation Officer
Tel.: +43 1 26030 6575
Email: *kevin.stickney@ctbto.org*

Ms Karin AL-BAKIR
Documentation Clerk
Tel.: +43 1 26030 6388
Email: *karin.al-bakir@ctbto.org*

Mr Gordon VACHON
Consultant
Tel.: +43 1 26030 6189
Email: *glvachon@gmail.com*

Logistics and Operational Support Section

Mr Bela BALCZO
Chief
Tel.: +43 1 26030 6473
Email: *bela.balczo@ctbto.org*

Equipment Section

Mr Rainier ARNDT
Chief
Tel.: +43 1 26030 6169
Email: *rainier.arndt@ctbto.org*

Mr Peter LABAK
Equipment and Implementation Officer
Tel.: +43 1 26030 6247
Email: *peter.labak@ctbto.org*

Training Section

Mr Mordechai MELAMUD
Chief
Tel.: +43 1 26030 6173
Email: *mordechai.melamud@ctbto.org*